Prime

An integer p greater than 1 is called prime if the only positive factors of p are 1 and p.

The primes are 2, 3, 5, 7, 11, 13, 17, 19, ...

The largest known prime number (as of August 2019) is $2^{82,589,933} - 1$, a number which has 24,862,048 digits.

It was found by Patrick Laroche of the Great Internet Mersenne Prime Search (GIMPS) in 2018.

The Fundamental Theorem of Arithmetic

Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the primes are written in order of nondecreasing size.

Ex: The prime factorizations of 100, 641, 999 and 1024 are given by

$$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 5^2$$

$$641 = 641$$

$$999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$$

$$1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$$

Thm:- If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

Ex: Show that 101 is prime.

The only primes not exceeding $\sqrt{101}$ are 2, 3, 5 and 7. Because 101 is not divisible by 2, 3, 5 and 7, it follows that 101 is prime.

Ex: Find the prime factorization of 7007

To find the prime factorization of 7007, first perform divisions of 7007 by successive primes, beginning with 2. None of the primes 2, 3 and 5 divides 7007. However, 7 divides 7007 with 1001.

Next, divide 1001 by successive primes, beginning with 7. It is immediately seen that 7 also divides 1001, because $\frac{1001}{7} = 143$.

Continue by dividing 143 by successive primes, beginning with 7. Although 7 doesn't divide 143, 11 does divide 143 and $143/11 = 13$. Because 13 is prime, the procedure is completed.

$7007 = 7 \cdot 7 \cdot 11 \cdot 13 = 7^2 \cdot 11 \cdot 13$.

large primes play a crucial role in cryptography

There is an ongoing quest to discover larger and larger prime numbers; for almost all the last 300 years, the largest prime known has been an integer of the special form $2^p - 1$, where p is also prime. Such primes are called Mersenne primes.

Greatest Common Divisors

Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and $d \mid b$ is called greatest common divisor of a and b. $\boxed{\gcd(a,b) = d}$

Ex: What is the gcd of 24 and 36?

Soln:- The positive common divisors of 24 and 36 are 1, 2, 3, 4, 6 and 12. $\gcd(24, 36) = 12$.

If $a = p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_n^{a_n}$; $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$ then $\gcd(a,b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}$